Docket No.: 08204/0203160-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
Kim F. Storm

Patent No.: 7,296,145

Issued: November 13, 2007

For: METHOD OF SECURE COMMUNICATION
OVER A DISTRIBUTED NETWORK
WITHOUT USING SECURE SOCKET LAYER

REQUEST FOR CERTIFICATE OF CORRECTION
PURSUANT TO 37 CFR 1.323 AND 1.322

Attention: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Upon reviewing the above-identified patent, Patentee noted typographical errors which should be corrected. A listing of the errors to be corrected is attached.

The typographical errors marked with an "A" on the attached list are found in the application as filed by applicant. Payment in the amount of $100.00 covering the fee set forth in 1.20(a) is enclosed.

The typographical errors marked with a "P" on the attached list are not in the application as filed by applicant. Also given on the attached list are the documents from the file history of the subject patent where the correct data can be found.

The errors now sought to be corrected are inadvertent typographical errors the correction of which does not involve new matter or require reexamination.

Transmitted herewith is a proposed Certificate of Correction effecting such corrections. Patentee respectfully solicits the granting of the requested Certificate of Correction.

The Commissioner is authorized to charge any deficiency of up to $300.00 or credit any excess in this fee to Deposit Account No. 04-0100.

Dated: December 10, 2007

Respectfully submitted,

By (53,970)

Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,296,145 Page 1 of 1

APPLICATION NO.: 09/853,743

ISSUE DATE : November 13, 2007

INVENTOR(S) : Storm

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 2, line 11, delete "Interjak™" and insert - - InterJack™ - -, therefor.

In column 6, line 35, in Claim 22, after "claim 21" insert - - wherein - -.

MAILING ADDRESS OF SENDER (Please do not use customer number below):
John W. Branch, Esq.
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770

Darby & Darby

Issued Patent Proofing Form File#: **08204/0203160-US0**

Note: P = **PTO Error** A = **Applicant Error**

US Serial No.: **09/853,743** US Patent No.: **US 7,296,145 B1** Issue Dt.: **Nov. 13, 2007**

Title: **METHOD OF SECURE COMMUNICATION OVER A DISTRIBUTED NETWORK WITHOUT USING SECURE SOCKET LAYER**

Sr. No.	P/A	Original		Issued Patent		Description Of Error
		Page	Line	Column	Line	
1	P	Page 4 Specification (05/10/2001)	13	2	11	Delete "Interjak™" and insert - - InterJack™ - -, therefor.
2	A	Page 6 Claims (08/09/2007)	Claim 22 Line 1	6	35	In Claim 22, after "claim 21" insert - - wherein - -.

METHOD OF SECURE COMMUNICATION OVER A DISTRIBUTED NETWORK WITHOUT USING SECURE SOCKET LAYER

BACKGROUND

1. Field of the Invention

The invention relates to network communication. More specifically, the invention relates to secure communication between network devices without the use of secure socket layer.

2. Background

With the proliferation of the internet, the need and desirability of managing devices over a distributed network in a secure manner continues to increase. Typical web browsers support Java, Java Script, frames and forms. However, the contents of such frames, forms, and even the Java Script passed between a web browser and a web server is typically freely visible to potential third parties snooping the web traffic. To ensure proper management and to avoid intentional and unintentional acquisition of sensitive data by third parties, the exchange between a browser and a device under management, should be secure, e.g., both authenticated and encrypted.

To permit secure communication between network nodes, Secure Socket Layer ("SSL") was developed by Netscape Communications Corporation as a protocol to permit encrypted communications. SSL is layered under Hypertext Transfer Protocol ("HTTP") and Above Transmission Control Protocol/Internet Protocol ("TCP/IP"). SSL is used by HTTPS as access methods. Unfortunately, SSL requires third party authentication, embedded certificates and exchange of certificates when the host name is changed. For these and other reasons, it is not suitable for management of embedded network appliances or certain other environments in which secure communication is desirable.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated by way of example and not by way of limitation in the figures of the accompanying drawings in which like references indicate similar elements. It should be noted that references to "an" or "one" embodiment in this disclosure are not necessarily to the same embodiment, and such references mean at least one.

FIG. **1** is a block diagram of the system of one embodiment of the invention.

FIG. **2***a* is a schematic diagram of the frames sent from a Device Under Management in one embodiment of the invention.

FIG. **2***b* is a schematic diagram representative of a layout for a concatenated string for one embodiment of the invention after decryption.

FIG. **3** is flow diagram of operation on the Device Under Management in one embodiment of the invention.

FIG. **4** is a flow diagram of operation on external node in one embodiment of the invention.

DETAILED DESCRIPTION

FIG. **1** is a block diagram of the system of one embodiment of the invention. A Device Under Management ("DUM") **100** is coupled to a distributed network such as internet **102**. External node **104** is also coupled to internet **102**. External node **104** may be used to manage DUM **100** over the internet **102**. There may be an arbitrarily large number of DUM's coupled with the internet **102** up to DUM_N **108** with each device manageable by external node **104**.

In one embodiment, external node **104** may be any internet access device that supports Java, Java Script, frames and forms. In one embodiment, external node **104** may be a personal computer (PC) executing a web browser such as Microsoft Explorer® or Netscape Navigator®. As previously noted, such browsers support Java, Java Script, frames and forms. DUM **100** may be any network element including an embedded network appliance, such as the Interjak™ 200 available from Filanet Corporation of Sunnyvale, Calif. DUM **100** may provide web server functions, or for example, a fire wall for clients **106**.

When external node **104** first requests secure access to DUM **100**, such as, for example, management access, device **100** serves a frame containing an embedded security applet to external node **104**. In one embodiment, the security applet is a Java applet. In another embodiment, the security applet may be realized using embedded Java Script code. The security applet generates a login window on the external node **104**. A user can then enter their required login data to gain access to the DUM **100**. As used herein, "login data" may include a user I.D., a password, or both. The security applet encrypts the login data and sends the encryption login data over the internet **102** to DUM **100**. In one embodiment, the login data is encrypted with a random key generated in DUM **100** and sent to the external node as part of the Java Script code within the login page. DUM **100** decrypts the login data and determines if the login data is valid. If the login data is valid, it is used as a basis for a key for all subsequent encryption. As used herein to serve "as a basis for the key" is deemed to include, without limitation, direct usage as the key, usage of all or part of the login data as a seed for a pseudo random number generator to generate a pseudo random key, and indirect use, such as using the login data to encrypt a known data set and using the encrypted known data set as the key for subsequent encryption or using a hash of the login data as the key. When the login data is used directly, longer login data will yield stronger encryption.

Subsequent pages are provided to the external node **104** as subframes of the frame containing the security applet. Such subframes include the form having blank fields, a concatenated string of the field values with a digital signature all separated by appropriate delimiters and encrypted using the login data based key, and a script to decode and distribute the string. In one embodiment, the script is a Java Script. In one embodiment, 3DES (3 Data Encryption Standard) encoding is used. In one embodiment, the encoded string is transferred into the Java Script section of the web page together with a Java Script to decode the string and distribute it to the fields appropriately. If the user modifies the fields at the external node **104**, the script provided as part of the page will concatenate at least the modified fields, digitally sign and encrypt the concatenated string. In one embodiment, only the modified fields are concatenated. In an alternative embodiment, all field values are concatenated if any field is modified. In one embodiment, the Java Script hooks into the security applet which performs the heavy lifting of the encrypting and signing function.

FIG. **2***a* is a schematic diagram of the frames sent from a Device Under Management in one embodiment of the invention. Parent frame **200**, which has resident security applet (not shown), remains active on the external node for the entire secure session. As explained below, by retaining login data and using that data as a key basis for encryption

8. The method of claim 6 wherein the security applet is a locally executed applet to perform decryption of the string subsequently sent using a key word from the login data.

9. The method of claim 6 further comprising:

comparing the login data to a valid login data to identify if the user is valid; and

denying access if the user node is not valid.

10. An internet access device having executable instructions that when executed, perform actions comprising:

accepting a frame having a resident security applet;

receiving a subframe including a form with a plurality of blank fields;

receiving an encrypted string of concatenated data;

locally decrypting the encrypted string with the security applet; and

distributing a plurality of portions of the decrypted string to the plurality of blank fields in the form.

11. The internet access device of claim 10 wherein distributing comprises:

parsing the string delimited by embedded length and data type.

12. The internet access device of claim 10 further comprising:

accepting user modification of a field in the form;

concatenating data into a string from at least one of the plurality of fields, including at least a content of the field modified;

encrypting the string using the security applet; and

transmitting the string to a remote node.

13. The internet access device of claim 10 further comprising:

deriving a key from login data supplied by a user.

14. The internet access device of claim 12 wherein an encryption key is based on login data received from a user.

15. The internet access device of claim 10 further comprising:

generating a login window within the frame;

receiving login data from a user; and

receiving the login data in the security applet.

16. A computer readable storage media containing executable computer program instructions which when executed cause a digital processing system to perform a method comprising:

concatenating data for a plurality of fields of a requested web page into a string;

encrypting the string;

serving to a user node, the web page and a form corresponding to the requested web page that includes a blank field in each of the plurality of fields and the encrypted string; and

enabling at least the encrypted string to be locally decrypted and distributed into each respective blank field at the user node.

17. The computer readable storage media of claim 16 which when executed cause a digital processing system to perform a method further comprising:

appending a digital signature to the string prior to encryption.

18. The computer readable storage media of claim 16 which when executed cause a digital processing system to perform a method further comprising:

inserting the string and a script into a defined portion of the web page to be served.

19. The computer readable storage media of claim 18 which when executed cause a digital processing system to perform a method further comprising:

the defined portion is a locally executed script section of the web page.

20. The computer readable storage media of claim 16 which when executed cause a digital processing system to perform a method further comprising:

serving a script within the web page, the script to decrypt the string and apportion the string to the blank fields.

21. The computer readable storage media of claim 16 which when executed cause a digital processing system to perform a method further comprising:

serving a security applet to the user node; and

receiving login data from the user node encrypted by the security applet.

22. The computer readable storage media of claim 21 the login data forms a basis for a key used to encrypt the string.

23. The computer readable storage media of claim 21 wherein the security applet is a locally executed applet to perform decryption of the string subsequently sent using a key word from the login data.

24. The computer readable storage media of claim 21 which when executed cause a digital processing system to perform a method further comprising:

comparing the login data to a valid login data to identify if the user is valid; and

denying access if the user node is not valid.

* * * * *